Intrusion Prevention System Release Notes

Version 3.9.0

Released: December 2016

Updated: January 2017

This document contains release-specific information for the TippingPoint Intrusion Prevention System (IPS) TippingPoint Operating System (TOS). The release notes describe new features and changes included in this release. This document is intended for system administrators, technicians, and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint IPS devices and associated devices.

To ensure that you have the latest version of the release notes and other product documentation, download these documents from the Threat Management Center (TMC) at *https://tmc.tippingpoint.com*, or contact your TippingPoint representative.

This document contains the following important information:

New and changed in this release

This release includes the following new features.

Stacking

Stacking enables you to increase the overall inspection capacity of your IPS by grouping multiple NX Series devices and pooling their resources.

You can configure up to five NX Series devices in a stack. The stack operates as a single device that you manage on the TippingPoint Security Management System (SMS). Devices in the stack must be the same model, either all 7100NX devices or all 7500NX devices.

In-line inspection capacity increases with each device that you add to the stack. For example, for each 7500NX added to a stack of 7500NX devices, the inspection capacity increases by 20 Gbps.

The following TippingPoint software is supported for stacking:

- **TippingPoint SMS v4.5.0, or later** - Centrally manages each stack of devices.
- **TippingPoint IPS v3.9.0, or later** - Must be installed on each security device.

Note: No additional licensing is required to implement stacking.

For complete information about stacking, see the *NX Series Stacking Deployment Guide* on the TMC.

Export a Tech Support Report from an IPS device

In the SMS, you can collect diagnostic information from an IPS device by exporting a Tech Support Report (TSR). The TSR collects information from diagnostic commands and log files into a report that TippingPoint Technical Support can use to debug and troubleshoot the device.

Unlike a TSR created on the device by using the IPS Local Security Manager (LSM), the TSR exported by the SMS does not include snapshot information. However, you can create a snapshot from the SMS. For complete information about how you can export a TSR from the SMS, see the *Security Management System User Guide*.

Release restrictions

The following restrictions apply to this release.

TOS v3.9.0 and IPS devices

TOS v3.9.0 is available for the following TippingPoint devices.

Product name	HPE part number	Trend Micro part number
TippingPoint 660N	JC019A	TPNN0020
TippingPoint 1400N	JC020A	TPNN0023
TippingPoint 2500N	JC021A	N/A

Product name	HPE part number	Trend Micro part number
TippingPoint 5100N	JC022A	N/A
TippingPoint 6100N	JC577A	N/A
TippingPoint S2600 NX	JC874A	TPNN0026
TippingPoint S5200 NX	JC824A	TPNN0029
TippingPoint S6200 NX	JC873A	TPNN0031
TippingPoint S7100 NX	JC644A	TPNN0034
TippingPoint S7500 NX	JC872A	TPNN0037

TOS v3.9.0 and Digital Vaccine (DV)

TOS v3.9.0 uses v3.2.0 DV packages.

TOS v3.9.0 and the SMS

SMS-managed devices with TOS v3.9.0 installed must be managed with SMS v4.5.0 or later. The SMS must be updated before you use it to manage devices with TOS v3.9.0 installed. Refer to the SMS release notes for information about updating the SMS.

TOS v3.9.0 and NTP

The following restriction applies to N-series devices only: Enabling NTP and then switching to SNTP causes the SNTP feature to fail. After switching from the NTP feature to SNTP or the Manual/Internal Clock, reboot the device for the change to take effect. (107814)

Supported transceivers and cables for TippingPoint I/O modules

Table 1. Supported transceivers for I/O modules

I/O module & part number	Transceiver part number	Transceiver name
6-Segment GbE SFP (TPNN0068)	TPNN0054	TippingPoint X126 1G SFP RJ45 Transceivers (Copper and Fiber)
4-Segment 10GbE SFP+ (TPNN0060)	TPNN0057 TPNN0058 TPNN0054	TippingPoint S136 10G SFP+ LC SR Transceiver TippingPoint S136 10G SFP+ LC LR Transceiver TippingPoint X126 1G SFP RJ45 Transceivers (Copper and Fiber)
1-Segment 40 GbE QSFP+ (TPNN0069)	TPNN0067	TippingPoint S146 40G QSFP+ SR4 850nm Transceiver

Table 2. Supported module cable

I/O module part number	Cable part number	Cable name
TPNN0069*	TPNN0212	TippingPoint 40G QSFP+ Active Optical Cable (AOC)

*When this I/O module is used with this cable, then transceiver TPNN0067 is not needed. The cable has the transceiver attached.

Installation

All devices must be running a minimum of TOS v3.7.2 before they can be upgraded to TOS v3.9.0.

Before upgrading your device to the latest TOS, maximize the space on your device by removing old TOS versions and packet traces. This ensures a successful upgrade and allows for a TOS rollback, if necessary.

You can remove previous TOS versions using the SMS, the LSM, or the CLI. For complete information, refer to the corresponding documentation on the TMC, *https://tmc.tippingpoint.com/TMC/*.

Resolved issues

The following items provide clarification or describe issues fixed in this release.

Description	Reference
Invalid characters in domain name Invalid characters were not restricted when the user created a domain name for a reputation group in the command-line interface (CLI). An error message now appears in the CLI when the Reputation domain name contains an invalid character.	106490
Blocked streams discrepancy with TRHA partner device The amount of blocked streams between an active IPS and its Transparent HA (TRHA) partner did not match. The active IPS showed a much larger number than the partner.	108363
Vulnerability scanner issue with the system log When the IPS was scanned by a McAfee vulnerability scanner, the IPS stopped logging system log messages and reported the following critical error: `System Log files disabled. Reset System Log to re-enable.` The system log now resets and logs new entries without a device reboot.	113061
System log flooded with warning messages The following message appeared too frequently and flooded the system log: `<WARN> [ NP] <AR0 > IP REP: Failed to update entry - removing from hit cache - expect pending behavior on future appearances of this address` The severity of this message was changed to INFO to resolve this issue.	113072
ZPHA discrepancy between N Series and NX Series devices After a reboot, the ZPHA state on N Series devices was different than on NX Series devices.	113407

Description	Reference
Now, if you manually change the ZPHA state to bypass on either N Series or NX Series devices, the state persists after you reboot the device, and the IPS correctly continues to bypass traffic. **Note:** If the ZPHA state is **not** manually changed to bypass, the state will be normal after a reboot.	

System log flooded with error messages
The following error message appeared too frequently and flooded the system log:
`<ERR> [NP] Could not create directory /user/XXX/log/pkt to hold adaptive filter config. dump files`
This message now appears fewer times in a row in the system log. The message text was also updated to the following:
`<ERR> [NP] Could not create directory to hold adaptive filter configuration temp files`
	114084

The following CVEs were addressed in this release: • CVE-2014-9750 • CVE-2015-5219 • CVE-2015-5300 • CVE-2015-3405 • CVE-2015-5146 • CVE-2015-3197 • CVE-2016-0701	114411, 114412, 114413, 111075, 111819
After the device was upgraded to TOS v3.8.4, filter 7173 incorrectly blocked traffic. This filter issue has been fixed.	114489

Known issues

This release contains the following known issues.

Description	Reference
RADIUS authentication issues • Certificate Notification — The LSM does not give an indication when no certificates are present on the device. • Microsoft Windows servers and EAP-MD5 authentication — Certain versions of the Microsoft Windows server do not accept EAP-MD5 authentication. For information on enabling this authentication, refer to the Microsoft Knowledge Base: *http://support.microsoft.com/kb/922574/en-us*	95399
Remote authentication system-level settings and user access The system-level setting determines the protocol that is used to authenticate all remote users for remote servers (**System > Remote Servers** on the LSM). Even though a user can be configured with a specific remote authentication protocol (RADIUS or TACACS+), the system-level setting for remote servers will be used during authentication with the remote servers.	101704
Scan/sweep filters Scan/sweep filters do not trigger, even after other filters are disabled. **Workaround**: This issue is less likely to occur if the scan/sweep filters are set to Block+Notify instead of Permit+Notify. Reboot the device after changing the filter from Permit+Notify to Block+Notify.	108666
Rate limit report The data for some devices is not displayed when the SMS runs a rate limit report.	115799
Link Down Synchronization wait time The Link Down Synchronization wait time can be set to any value from 0 to 240 seconds; however, the wait time always takes at least 3 seconds.	115957
I/O module configuration restrictions when stacking is enabled	116208

Description	Reference
When stacking is enabled, do not make the following configuration changes to the slot 4 I/O module segments: • Enable link-down synchronization • Configure VLAN translation rules • Configure inspection bypass rules • Enable and disable ports	
Removing a device from a stack If you remove a device from a stack, you can repurpose it for use in another stack or as a standalone device. To repurpose a device, you must use the `debug factory-reset` command. This restores the device to its original settings.	116325
Restoring a stacked device snapshot to standalone device If you restore a stacked device snapshot to a standalone device, the device state will be invalid. **Workaround**: Use the `reboot -full` command to put the device back into a valid state.	116397

OpenSSH version 7.2 or later
Newer versions of OpenSSH (v7.2 or later) no longer connect to the device by default because of an increase in the minimum number of bits for the key exchange.
Workaround:
• **Option 1**- Specify the key exchange parameter:
`ssh -o KexAlgorithms=diffie-hellman-group1-sha1 <ip_address>`
• **Option 2**- Ensure that SSH works without special parameters by placing the device into FIPS crypto mode:
`conf t host fips-mode crypto`
Note: A device reboot is required after using this command.
	116548

Description	Reference
IPv6 and SNMPv3 When a device is configured with IPv6 and SNMPv3 support is enabled, a trap destination configured with an IPv6 address causes traps to be sent to the incorrect UDP port. **Workaround**: Use an IPv4 address instead of IPv6.	116584

Product support

Get support for your product by using any of the following options:

Email support

tippingpoint.support@trendmicro.com

Phone support

North America: +1 866 681 8324

International: See *https://tmc.tippingpoint.com*

Legal and notice information

Intrusion Prevention System Release Notes

Edition: December 2016

Publication Part Number: 5998-1406